



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

Am

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/652,454	08/31/2000	David Cheriton	CISCP537	3379
26541	7590	05/25/2005	EXAMINER	
RITTER, LANG & KAPLAN P.O. BOX 2448 SARATOGA, CA 95070			SIMITOSKI, MICHAEL J	
			ART UNIT	PAPER NUMBER
			2134	

DATE MAILED: 05/25/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/652,454

Applicant(s)

CHERITON, DAVID

Examiner

Michael J. Simitoski

Art Unit

2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 04 April 2005.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1,3,4,6-21,23-30 and 32-36 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1,3,4,6-21,23-30 and 32-36 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. The response of 4/4/2005 was received and considered.
2. Claims 1, 3-4, 6-21, 23-30 and 32-36 are pending.

Response to Arguments

3. Applicant's arguments with respect to claims 1, 3-4, 6-21, 23-30 & 32-36 have been considered but are moot in view of the new ground(s) of rejection.
4. Applicant's response regarding claims 8 & 19 (p. 13, ¶4-5) argues that Brodnik teaches away from using hardware. However, Brodnik teaches a concept well known to one of ordinary skill in the art – hardware is generally faster than software, but less flexible (and hence software is slower, but more flexible). Thus, Brodnik teaches benefits of hardware and software as well as the disadvantages to both hardware and software. Because Brodnik gives disadvantages to both does not imply that Brodnik is teaching away from both, but rather that a tradeoff exists and both hardware and software are known to be advantageous. Further, all software is run on hardware and therefore any element that is performed in software is an element that is also performed on/comprised of hardware.

Claim Rejections - 35 USC § 112

5. The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

Art Unit: 2134

6. Claims 32-34 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention. The specification does not make clear to one skilled in the art how the flow analyzer is able to identify if a rate of traffic exceeds a sampling capability of the aggregate filter.

7. Claim 35 is rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. The specification does not disclose building new flow cache entries for network flows without a corresponding flow cache. *For the purposes of this Office Action, "without a corresponding flow cache" is understood to mean "without a corresponding flow cache entry".*

8. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

9. Claims 13 & 32-35 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Regarding claim 13, the limitation "high rate" is indefinite because it is a relative term.

Regarding claim 32, the claim recites the limitation "the aggregate filter" in line 3. There is insufficient antecedent basis for this limitation in the claim.

Regarding claim 33, an “aggregate filter” is recited in the depending claim 32 and therefore it is unclear if an additional aggregate filter is being claimed.

Regarding claim 35, it is unclear how new flow cache entries for network flows are built without a cache. *For the purposes of this Office Action, “without a corresponding flow cache” is understood to mean “without a corresponding flow cache entry”.*

Claim Rejections - 35 USC § 101

10. 35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

11. Claims 15-17 & 36 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Claim 15 is a computer product on a computer-readable storage medium, including a data signal embodied on a carrier wave.

Claim Rejections - 35 USC § 103

12. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

13. Claims 1, 3-4, 6-7, 9-13, 15-18, 20-21, 23-25, 27-30 & 35-36, as best understood, are rejected under 35 U.S.C. 103(a) as being unpatentable over WO 97/24841 to Cheriton et al. (**Cheriton**) in view of “Cisco Flow Logs and Intrusion Detection at the Ohio State University”

by Romig et al. (**Romig**) in view of “Operating Firewalls Outside the LAN Perimeter” by Smith et al. (**Smith**).

Regarding claims 1, 6-7, 9-10, 15-18, 21 & 35, Cheriton discloses classifying network flows/virtual paths based on one or more packets/datagrams received at the network device (p. 7, ¶2 & p. 8, ¶2-3), performing a lookup for each of the classified network flows/virtual paths (p. 8, ¶2) and building a new flow/virtual path cache entry if the lookup is unsuccessful (p. 8, ¶3), sending each of said network flows/virtual paths to a corresponding flow/virtual path cache (p. 8, ¶3), implementing policies designated for each of said network flows (p. 13, ¶5) and creating separate aggregate network flow summaries/virtual path records for each of said network flows/virtual paths (p. 10, ¶6 – p. 1, ¶2). Cheriton lacks creating separate aggregate network flow summaries for each of said network flows and analyzing at least one of said aggregate network flow summaries to detect characteristics of potentially harmful network flows.

However, Romig teaches that aggregating subsequent traffic in flow logs (p. 3, ¶2) is beneficial because they can be used for intrusion detection (analyze for potentially harmful flows) (p. 5, ¶1). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Cheriton to create separate flow summaries for each of said network flows. One of ordinary skill in the art would have been motivated to perform such a modification to allow for intrusion detection by examining the flow summaries, as taught by Romig (p. 3, ¶2 & p. 5, ¶1). As modified, Cheriton lacks generating a filter to prevent packets corresponding to detected potentially harmful network flows from passing through said network device. However, Smith teaches a firewall that works with intrusion detection software to automatically cause a set of firewalls to dynamically change security policy (generate filter) for

Art Unit: 2134

individual attack activity (p. 494, col. 1, ¶3) to push the protection to a point of finding the gateway nearer to the hacker (p. 496, col. 2, last ¶ & p. 498, ¶2). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Cheriton to generate a filter corresponding to detected potentially harmful network flows to prevent packets from passing through the network device. One of ordinary skill in the art would have been motivated to perform such a modification to push the protection to a point of finding the gateway nearer to the hacker, as taught by Smith (p. 494 col. 1 ¶3, p. 496 col. 2 last ¶ & p. 498 ¶2).

Regarding claims 3 & 4, Cheriton discloses classifying the network flow base on a source device sending a packet (p. 7, ¶2).

Regarding claims 11 & 25, Cheriton discloses selecting a class of flows/virtual paths to analyze based on previously analyzed paths (Cheriton, p. 8, ¶2-3 & Smith, p. 5, ¶1).

Regarding claims 12 & 13, Cheriton, as modified above, discloses denial of service attacks (Smith, §2.1) and a high rate of incoming packets (Smith, §2.1 & Romig, p. 7, ¶1).

Regarding claim 20, Cheriton, as modified above, discloses an ACL classifier/switch hardware (p. 13, ¶4 & Fig. 4), a lookup device/virtual path cache (p. 13, ¶4 & Fig. 4) and a plurality of flow buckets/shared buffer memory (p. 13, ¶3-4 & Fig. 4).

Regarding claim 23, Cheriton, as modified above, discloses reducing the flow summaries in hardware (Romig, p. 4, ¶1-3) so that the flow records can be analyzed by software/programs (Smith, p. 4, ¶5).

Regarding claims 24, 28-30 & 36, Cheriton, as modified above further teaches refining said filter (Smith, §3.3 #3 & p. 498 ¶2).

Regarding claim 27, Cheriton, as modified above, lacks a class of packets being selected for analysis based on statistics associated with an aggregate filter. However, Romig teaches that a class of packets (records pertaining to hosts) is analyzed (p. 5, ¶2) based on statistics (flow logs, reports) associated with an aggregate filter (flow-dscan results reports) (p. 5, ¶1). This allows a more thorough investigation to determine further whether a possible scan was actually a scan or not and to see whether there exists other questionable activity that should be investigated (analyzed) (p. 5, ¶2). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Cheriton to select a class of packets for analysis based on statistics associated with an aggregate filter. One of ordinary skill in the art would have been motivated to perform such a modification to more thoroughly investigate whether a possible scan was actually a scan or not and to see whether there exists other questionable activity that should be investigated/analyzed, as taught by Romig (p. 5, ¶1-2).

14. Claims 8 & 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Cheriton, Romig & Smith**, as applied to claims 1 & 18 above, in further view of U.S. Patent 6,266,706 to Brodник et al. (**Brodnik**). Cheriton, as modified above, discloses the analyzing step being performed by software/programs (Romig, p. 5, ¶5), but lacks the sending step being performed by hardware. However, Brodnik teaches that special-purpose hardware is useful for high-speed and software is used for flexibility (col. 2, line 64 – col. 3, line 3). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the system so the sending step is performed in hardware. One of ordinary skill in the art would have

Art Unit: 2134

been motivated to perform such a modification to make the sending step fast and the analyzing step flexible to change, as taught by Brodnik (col. 2, line 64 – col. 3, line 3).

15. Claim 14 is rejected under 35 U.S.C. 103(a) as being unpatentable over **Cheriton, Romig & Smith**, as applied to claim 1 above, in further view of U.S. Patent 6,389,532 to Gupta et al. (**Gupta**). Cheriton, as modified above, lacks explicitly identifying a source address associated with a harmful network flow and generating a filter to prevent packets from that source from passing through the network. However, Gupta teaches that a router can filter packets when a predetermined router limit, such as a rate at which a router may receive packets from a particular source, has been exceeded, to prevent denial of service attacks (col. 7 lines 28-52). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to identify a source of a harmful packet flow and generate a filter to prevent incoming packets from the source. One of ordinary skill in the art would have been motivated to perform such a modification to prevent denial of service attacks, as taught by Gupta (col. 7 lines 28-52).

16. Claim 26 is rejected under 35 U.S.C. 103(a) as being unpatentable over **Cheriton, Romig & Smith**, as applied to claim 1 above, in view of U.S. Patent 6,651,099 to Dietz et al. (**Dietz**). Cheriton, as modified above, lacks sending information on a selected group of flows to a classifier. However, Dietz teaches that to recognize a conversational flow associated with a particular applications, it is necessary to examine further packets and maintain a state of a flow (col. 10, lines 8-23). Packets are continually reclassified until a conversational flow (as opposed to a connection flows (col. 2, lines 34-48)) is satisfactorily identified (col. 10, lines 8-35).

Art Unit: 2134

Conversational flow recognition is useful because a single application may produce different “connection flows” (col. 3, lines 34-48). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to pass information on the selected group of network flows to a classifier. One of ordinary skill in the art would have been motivated to perform such a modification to recognize conversational flows, as taught by Dietz (col. 2, lines 34-48 & col. 10, lines 8-35).

17. Claims 32 & 34, as best understood, are rejected under 35 U.S.C. 103(a) as being unpatentable over **Cheriton, Romig & Smith**, as applied to claim 18 above, in view of U.S. Patent 6,667,985 to **Drummond-Murray**. Cheriton lacks identifying if a rate of traffic exceeds a sampling capability of the aggregate filter and a rate-limiting policer to prevent system overload. However, Drummond-Murray teaches that to reduce congestion, when an amount of traffic corresponding to a maximum capability is reached, the traffic is throttled (rate-limited) (col. 1, line 61 – col. 2, line 6 & col. 3, lines 26-48). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to identify if a rate of traffic exceeds a sampling capability and to include a rate limiter in Cheriton’s invention. One of ordinary skill in the art would have been motivated to perform such a modification to reduce congestion, as taught by Drummond-Murray (col. 1, line 61 – col. 2, line 6 & col. 3, lines 26-48).

Conclusion

18. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael J. Simitoski whose telephone number is (571) 272-3841.

Art Unit: 2134

The examiner can normally be reached on Monday - Thursday, 6:45 a.m. - 4:15 p.m.. The examiner can also be reached on alternate Fridays from 6:45 a.m. - 3:15 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached at (571) 272-3838.

Any response to this action should be mailed to:

Commissioner of Patents and Trademarks
Washington, DC 20231

Or faxed to:


(703)746-7239 (for formal communications intended for entry)

Or:

(571)273-3841 (Examiner's fax, for informal or draft communications, please label "PROPOSED" or "DRAFT")

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (571) 272-2100.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).


MJS
May 19, 2005


GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100